CLAIMS

1. A pseudorandom number generator (1) for generating a pseudorandom number sequence of a predetermined bit length, comprising:

a first linear feedback shift register (2) having **m** steps of shift registers to provide a bit string of a predetermined bit length;

a second linear feedback shift register (3) having **n** steps of shift registers to provide a bit string of a predetermined bit length;

an initial value generator (4) to generate, according to predetermined conditions, initial values for the respective shift registers of the first linear feedback shift register (2) and second linear feedback shift register (3) and supply the initial values to the first linear feedback shift register (2) and second linear feedback shift register (3);

a polynomial coefficient generator (5) to generate, according to predetermined conditions, coefficients of a characteristic polynomial of the second linear feedback shift register (3) and supply the coefficients to the second linear feedback shift register (3);

a primitive polynomial memory (8) to store a plurality of primitive polynomials with identification information representative of the primitive polynomials, one of the primitive polynomials serving as a characteristic polynomial of the first linear feedback shift register (2);

a primitive polynomial selector (7) to select, according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory (8) and supply coefficients of the primitive polynomial as coefficients of a characteristic polynomial to the first linear feedback shift register (2); and

a pseudorandom number output unit (6) to generate the pseudorandom number sequence of the predetermined bit length by carrying out bit-by-bit logical operations on the bit string provided by the first linear feedback shift register (2) and the bit string provided by the second linear feedback shift register (3) and output the pseudorandom number sequence.

2. The pseudorandom number generator as set forth in claim 1, wherein:

the pseudorandom number generator (1C) comprises a communication unit (9) to generate initial data including the identification information of the primitive polynomial selected by the primitive polynomial selector (7), the initial values generated by the initial value generator (4) for the shift registers of the first linear feedback shift register (2) and second linear feedback shift register (3), and the coefficients of the characteristic polynomial generated by the polynomial coefficient generator (5), send the initial data to a second pseudorandom number generator (1C), receive, if any, initial data from the second pseudorandom number generator (1C), extract from the received initial data initial values for the first linear feedback shift register (2) and second linear feedback shift register (3), supply the extracted initial values to the first linear feedback shift register (2) and second linear feedback shift register (3), extract coefficients for a characteristic polynomial from the received initial data, supply the extracted coefficients to the second linear feedback shift register (3), extract identification information of a primitive polynomial from the received initial data, and supply the extracted identification information to the primitive polynomial selector (7); and

the primitive polynomial selector (7) selects one of the primitive polynomials stored in the primitive polynomial memory (8) according to the identification information extracted by the communication unit (9) and supplies coefficients of the primitive polynomial to the first linear feedback shift register (2).

3. A pseudorandom number generation program executed by a computer to generate a pseudorandom number sequence of a predetermined bit length, the pseudorandom number generation program making the computer function as:

a first linear feedback shift register having **m** steps of shift registers to provide a bit string of a predetermined bit length;

a second linear feedback shift register having **n** steps of shift registers to provide a bit string of a predetermined bit length;

initial value generation means for generating, according to predetermined conditions, initial values for the respective shift registers of the first linear feedback shift register and second linear feedback shift register and supplying the initial values to the first linear feedback shift register and second linear feedback shift register;

polynomial coefficient generation means for generating, according to predetermined conditions, coefficients of a characteristic polynomial of the second linear feedback shift register and supplying the coefficients to the second linear feedback shift register;

primitive polynomial memory means for storing a plurality of primitive polynomials with identification information representative of the primitive polynomials, one of the primitive polynomials serving as a characteristic polynomial of the first linear feedback shift register;

primitive polynomial selection means for selecting, according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory means and supplying coefficients of the primitive polynomial as coefficients of a characteristic polynomial to the first linear feedback shift register; and

pseudorandom number output means for generating the pseudorandom number sequence of the predetermined bit length by carrying out bit-by-bit logical operations on the bit string provided by the first linear feedback shift register and the bit string provided by the second linear feedback shift register and outputting the pseudorandom number sequence.

4. The pseudorandom number generation program as set forth in claim 3, wherein:

the pseudorandom number generation program further makes the computer function as communication means for generating initial data including the identification information of the primitive polynomial selected by the primitive polynomial selection means, the initial values generated by the initial value generation means for the shift registers of the first linear feedback shift register and second linear feedback shift register, and the coefficients of the characteristic polynomial generated by the polynomial coefficient generation means, sending the initial data to a second pseudorandom number generator, receiving, if any, initial data from the second pseudorandom number generator, extracting from the received initial data initial values for the first linear feedback shift register and second linear feedback shift register, supplying the extracted initial values to the first linear feedback shift register and second linear feedback shift register, extracting coefficients for a characteristic polynomial from the received initial data, supplying the extracted coefficients to the second linear feedback shift register, extracting identification information of a primitive polynomial from the received initial data, and supplying the extracted identification information to the primitive polynomial selection means; and

the primitive polynomial selection means selects one of the primitive polynomials stored in the primitive polynomial memory means according to the identification information extracted by the communication means and supplies coefficients of the primitive polynomial to the first linear feedback shift register.